THE DIFFERENT USAGES OF SPLUNK

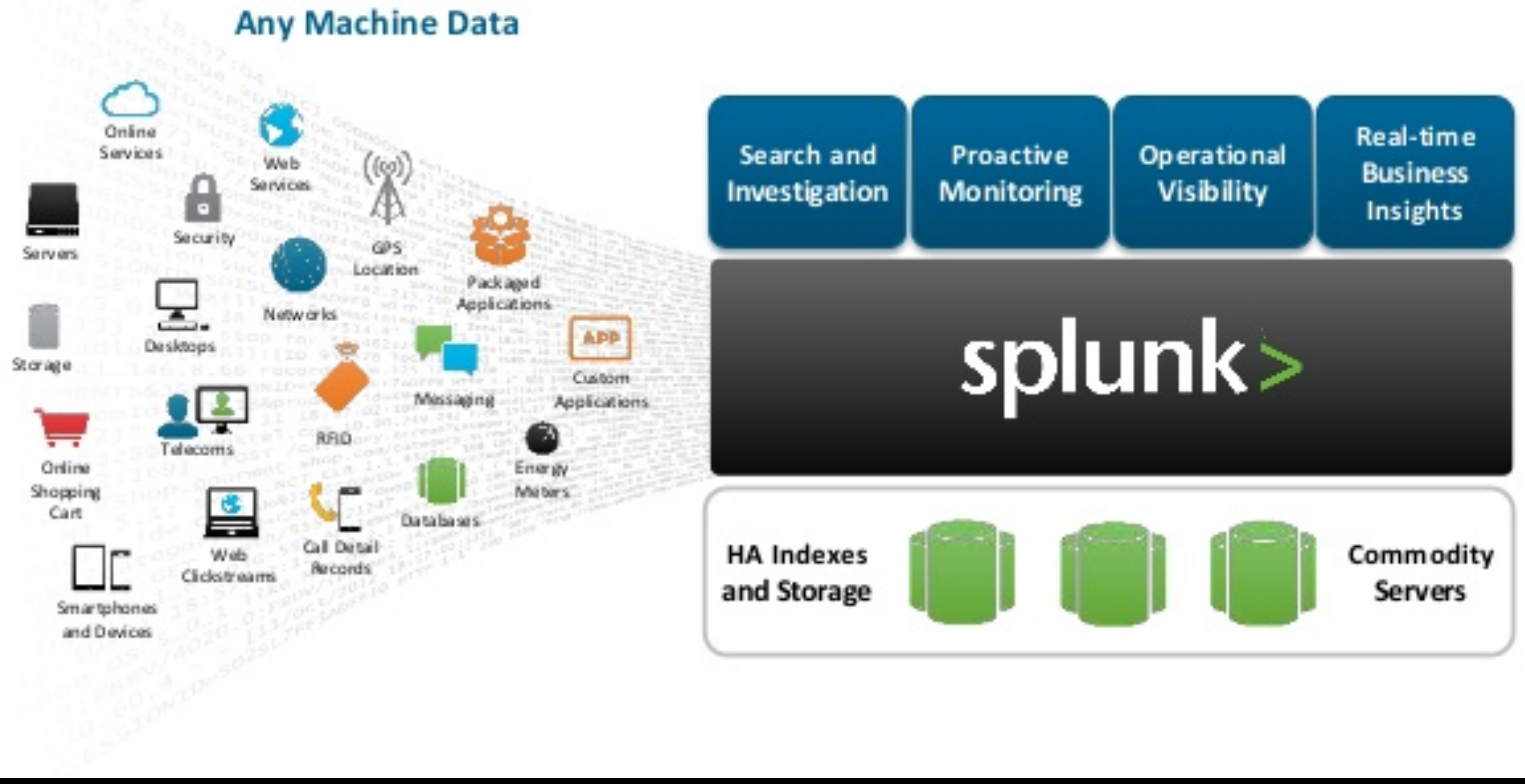
bilgehan.turan@eurocontrol.int
www.linkedin/in/bilgehanturan

EUROCONTROL

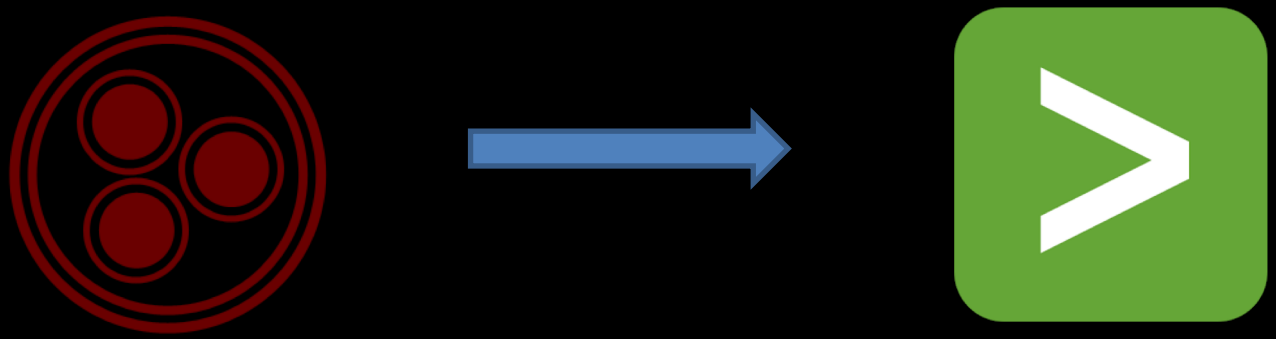
EATM-CERT
European Air Traffic Management
Computer Emergency Response Team

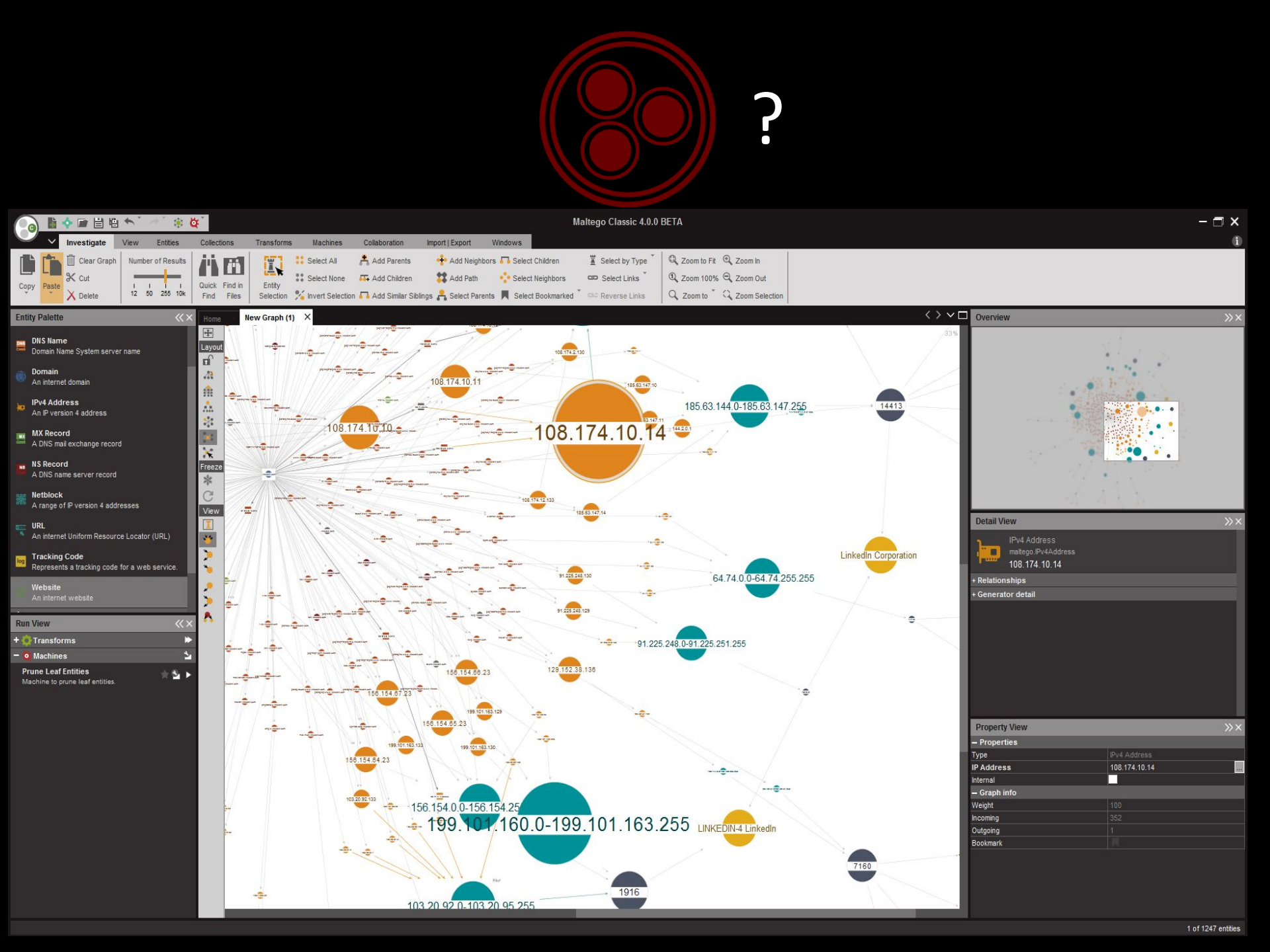
?

What is Splunk?



Use Case 1: Use with Maltego

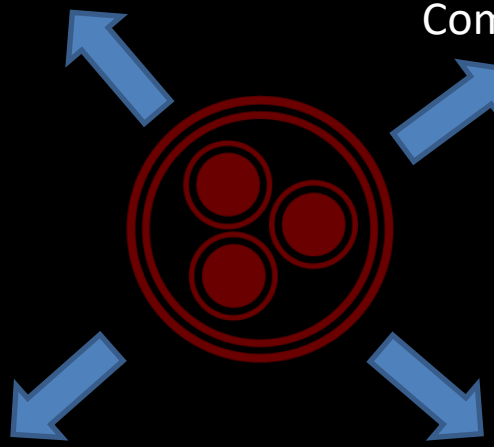



?
Maltego Classic 4.0.0 BETA
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
DNS Name
Domain Name System server name
Domain
An internet domain
IPv4 Address
An IP version 4 address
MX Record
A DNS mail exchange record
NS Record
A DNS name server record
Netblock
A range of IP version 4 addresses
URL
An internet Uniform Resource Locator (URL)
Tracking Code
Represents a tracking code for a web service.
Website
An internet website
Run View
Transforms
Machines
Prune Leaf Entities
Machine to prune leaf entities.
New Graph (1)
108.174.10.14
108.174.10.10
108.174.10.11
185.63.144.0-185.63.147.255
14413
LinkedIn Corporation
64.74.0.0-64.74.255.255
91.225.248.0-91.225.251.255
199.101.160.0-199.101.163.255
LINKEDIN-4 LinkedIn
156.154.0.0-156.154.25
103.20.92.0-103.20.95.255
7160
1916
Overview
Detail View
IPv4 Address
maltego.IPv4Address
108.174.10.14
Relationships
Generator detail
Property View
Properties
Type
IPv4 Address
IP Address
108.174.10.14
Internal
Graph info
Weight
100
Incoming
352
Outgoing
1
Bookmark
1 of 1247 entities

Maltego Components

Local Transforms

CTAS
Commercial Transform Application Server



iTDS
Internal Transform Distribution Srv

MDAS
Meta Data Application Server

Local Transform Demo

https://github.com/eatm-cert/maltego

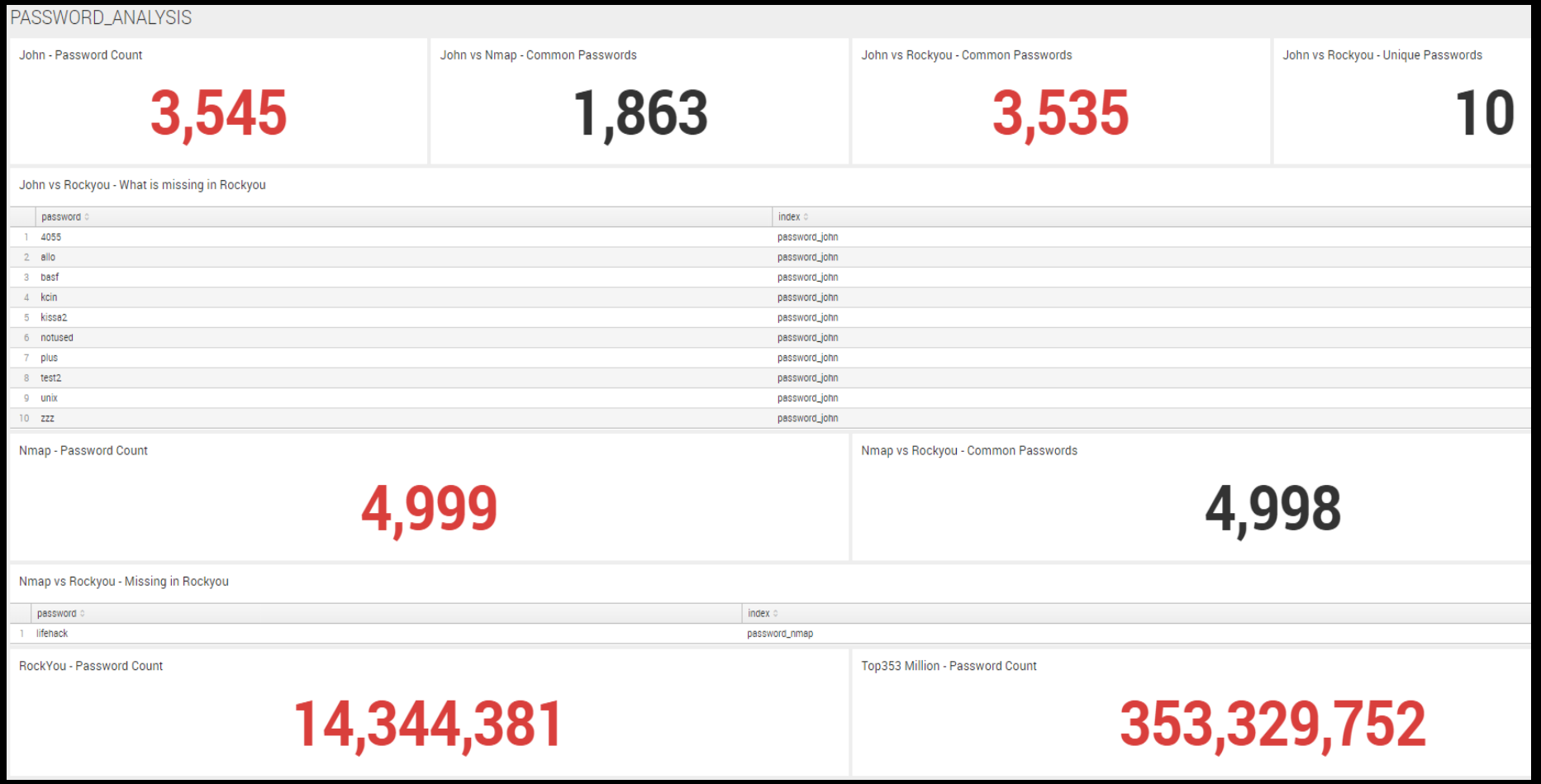
```
#!/usr/bin/python
import splunklib.client as client
import sys
from time import sleep
import splunklib.results as results
from MaltegoTransform import *
import os

HOST = "xxxxxx"
PORT = 8089
USERNAME = "xxxxx"
PASSWORD = "xxxxx"
AS=sys.argv[1] #define in maltego local transform commandline parameter as.number
# Create a Service instance and log in
service = client.connect(
    host=HOST,
    port=PORT,
    username=USERNAME,
    password=PASSWORD)

# Print installed apps to the console to verify login
#for app in service.apps:
#    print app.name

#edit search according to your splunk knowledge objects.
searchquery_normal = "search index=intelmq sourcetype=intelmqJSON source.asn="+ str(AS)+ " |  table source.ip |dedup source.ip | top limit=10 source.ip"
```

```
# Get the results and display them
me = MaltegoTransform()
for item in reader:
    #print "-----------------------------------------------"
    me.addEntity("maltego.IPv4Address",item['source.ip'])

me.returnOutput()


job.cancel()
```

Use Case 2: Wordlist Analysis

- John the ripper wordlist
- Nmap wordlist
- Kali – Rockyou wordlist
- Top353 million (not deduplicated) (https://github.com/berzerk0)

Analiz Dashboard



Comparison:John vs ...

John - Password Count

3,545

John vs Nmap - Common Passwords

1,863

John vs Rockyou - Common Passwords

3,535

John vs Rockyou - Unique Passwords

10

John vs Rockyou - What is missing in Rockyou

	password
1	4055
2	allo
3	basf
4	kcin
5	kissa2
6	notused
7	plus
8	test2
9	unix
10	zzz

Comparison:Nmap vs …

Nmap - Password Count

4,999

Nmap vs Rockyou - Common Passwords

4,998

Nmap vs Rockyou - Missing in Rockyou

	password
1	lifehack

Comparison:Rockyou vs …

RockYou - Password Count

14,344,381

Top353 Million - Password Count

353,329,752

	_raw	count
1	john	4,501.00
2	david	3,285.00
3	mike	3,021.00
4	mark	2,906.00
5	chris	2,663.00
6	james	2,449.00
7	michael	2,282.00
8	joe	2,186.00
9	jason	2,091.00
10	matt	2,045.00

Other Usages

- Integrate applications that checks passwords whether it is in wordlists or not during password change process
- Import Maltego Investigation graph to Splunk
  - Save investigations to monitored path

Some Usefull Queries

- set intersec|union|diff [subsearch] [subsearch]
- index=password_john OR index=password_nmap| stats count as common by _raw| stats count(eval(common==2)) as commoncount
- index=password_* |dedup _raw|fields -_*|fields _raw| outputcsv deduped_wordlists.csv

Some Limitations

- 10k items can be sorted, others truncated
  - Sort 0 <field>
- Subsearch 10k event limitation
  - Limits.conf → [subsearch] → maxout (upto 50K)
- Search output limitation = 10GB
  - $SPLUNK_HOME/etc/system/default/authorize.conf → srchDiskQuota
- Set operations → 10K since it uses subsearch

Conclusions

- With Splunk API, you can search your logs and use results in any application
- You can easily analyse huge data and extract useful information


THANK
YOU